To achieve this goal, the Infosec-tree structure facilitates the process of applying security design principles [13], and security patterns [23] in a natural and intuitive way. Multiple lines of defense, layered design, or diversity of mechanisms strategies can be easily applied using the nested structure of components represented by the Infosec-tree.

Upper-level nodes can provide common and general security mechanisms to all their contained components, and lower-level nodes can specify more specific and specialized security controls.

Furthermore, end-point connections are good places to apply strategies such as least privilege, least common mechanism, separation of privilege, or more complex patterns like virtual private network. For internal nodes, we can consider strategies like fail-safe defaults, complete mediation, economy of mechanism, open design, and more.

How and where these principles and patterns are applied to the tree is going to depend on the specific system and security requirements, but the proposed tree structure contributes positively to engage and implement them during the assurance process.

Consider one more time the data center example of Fig. 1, and the following confidentiality policy, *information owned or guarded by the organization should be accessed only by authorized people. If there is doubt about authorization, access should be denied*. Suppose that we want to protect information for confidentiality while is stored, processed or transmitted. Having a root node to represent the entire data center, we can install a security countermeasure to satisfy this requirement at the root node. This countermeasure is going to protect all the information contained in the corresponding component. But we can also implement additional confidentiality controls for the subcomponents of the data center, i.e. servers, switching device, storage, and recursively apply the same process to the subcomponents of these components.

Now, suppose that we want to apply the same confidentiality policy to a web application running inside a small group of virtual servers, contained in a blade server of the data center. We can use firewall rules at each of the virtual servers to control internal communications between them. But can go one level up, and define a firewall at the network level to control that communication. We can also use both controls, to provide different granularity levels of isolation.

After establishing the security services for the nodes, next step is to create security triads. We have to define the assurance moment (protection, detection, response), the information state (storage, processing, transmission, creation, destruction), and the security service for each triad. To finish this step, we associate an appropriate countermeasure to each triad, according to the security designer decision and to the available security resources. Fig. 2b and Fig. 2c show triad examples with associated countermeasures.

2.3.4. Step 4 – Assuring security controls. This final step is a complimentary process to verify the security of the security countermeasures installed after executing the previous methodology steps. Newly added security components can bring new vulnerabilities for several reasons. They can be complex systems requiring configuration, such as an intruder detection system. They may not be properly configured, or they can have vulnerabilities from factory, that we have to patch before production.

For example, a corporate antivirus platform typically requires some tuning, and periodic maintenance to preserve their integrity and correct functionality. A similar case happens with appliances and security devices that require software, or firmware updates, to fix vulnerabilities, and other functional and security issues.

The process to assure the security countermeasures, when required, starts by adding them to the Infosec-tree. They have to be located in the tree accordingly, like any other component of the system.

After including the security controls in the tree, we have to execute step 3 of methodology for each of them, namely establishing security services, security triads and countermeasures, like any other component of the system.

Next section describes a case study for Infosec-tree model, and some results from applying the methodology to the UCR Academic Cloud.

3. Study Case: Academic Cloud at UCR

UCR is the largest and most important public university in Costa Rica. Established in 1940, it has defined goals for education, research and social welfare. UCR academic cloud is an institutional research project started on 2013 to provide the academic and administrative communities at the University with a private cloud computing infrastructure.

Current installed hardware platform has more than 80 half height HP blade servers. Each server contains two eight-core processors, 128 Gbytes RAM, and two 146 Gbytes SAS RAID-1 configured hard disks.

Networking infrastructure connects the cloud to the campus network. It includes two HP 12500 Switches with optional Software Defined Networking (SDN) capabilities. These devices provide fault-tolerant and scalable operation with a throughput of 24.3 Tbps.

Cloud storage is powered by an EMC VNX 5700 with a hierarchical disk structure of NL-SAS, SAS, and SSD hard disks, and a raw estimate capacity of 400 TBytes. Storage components provide unified storage for files, blocks and objects, de-duplication, compression and thin provisioning for capacity improvement.

We have chosen this infrastructure to test our methodology because of its complexity and diversity of security requirements. In this section, we describe some real use cases extracted from our security solution for this cloud.

3.1. Information Security Policies

Security policies are the starting point of the assurance process. They are used as the input to apply the methodology. The following is a subset of the security policies at UCR.

1. *Confidentiality policy*: information owned or guarded by the UCR should be accessed only by authorized people. If there is doubt about authorization, access should be denied.
2. *Integrity policy*: information stored, transmitted or processed by the UCR systems, and by the effects considered its property cannot be under any circumstances modified or eliminated, without having formal authorization by the authorized personnel.
3. *Availability policy*: the UCR will provide a continuity plan to reduce the effect of interruptions, so availability of resources and services can be maximized, according to the possibilities of the institution.
4. *Authentication policy*: information stored, transmitted or processed by the UCR systems, and by the effects considered its property cannot be under any circumstances be accessed without authentication of authorized staff.

3.2. Case Analysis

Use cases explained in this section are representative of the assurance process, but they are partial examples. They describe only a small number of the required security services for the real platform. The full process generates extensive documentation that cannot be included in this article.

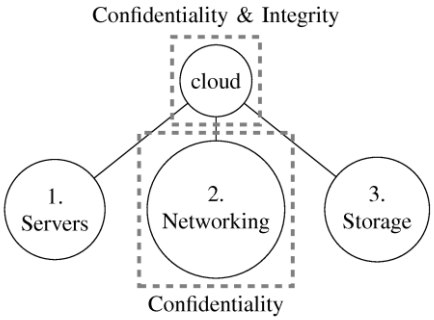
We start with a high level example describing the root element of the Infosec-tree, and then it comes with more detailed examples.

3.2.1. Case Analysis for the Top Level Component. The first case considers the two upper-levels of the Infosec-tree. Our cloud is composed of a set of servers, networking devices and storage devices, as shown in Fig. 4a.

Our goal is to protect information being transferred in or out of the cloud for confidentiality (policy 1), and also to protect information being transferred inside the cloud for integrity (policy 2).

We can apply security mechanisms at the root node, and also enforce confidentiality at the networking devices. Although, we considered confidentiality and integrity for Servers and Storage, we decided to use the mechanisms at lower-level sub-nodes. The resulting partial Infosec-tree is shown in Fig. 4a.

Now, we can define security triads and countermeasures at the entry point of the cloud. For information coming in and out we have the end-point and the triads shown in Fig. 4b and Fig. 4c, respectively. These triads propose a firewall for confidentiality, and an intrusion prevention system



(a) Infosec-tree for the cloud study.

(b) Cloud infosec-node.

End-point a
(protection, transmission, confidentiality) → firewall
(protection, transmission, integrity) → intrusion prevention system

(c) End-point table for Cloud infosec-node.

Figure 4. Case analysis for the cloud component.

(IPS) for integrity. We can install these devices at the entry point of the cloud to enforce the security policies.

From the example we can see that not every end-point has a connecting peer inside the system, namely another component to communicate that belongs to the system. In this case the other end is an external network, mostly the Internet, connected to the cloud data center.

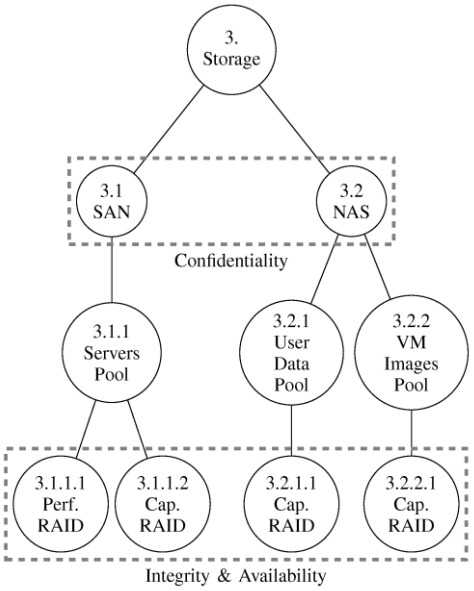
2.3.4. Case Analysis for Storage. This case shows how the whole-parts pattern can be applied into the tree for logical components, as opposed to physical components. The Storage sub-tree shown in Fig. 5a proposes confidentiality, integrity and availability services (policies 1, 2, and 3).

Storage node is composed of two logical subcomponents, namely Storage Area Network (SAN) for local storage, and Network-Attached Storage (NAS) for network storage. They require confidentiality because we want to allow storage access only for blade servers located in the data center, and not for external servers.

About integrity and availability, the hardware capabilities of the storage provide a “pool” abstraction, which allows defining groups of disks, assigned by demand, and they are composed of one or more arrays of physical disks. The hardware also provides RAID technology for arranging the disks. Then, we used these facilities to satisfy the security requirements for integrity and availability.

Fig. 5a shows several types of arrays, such as Performance (Perf. RAID), and Capacity (Cap. RAID), for faster access or larger capacity, respectively. Fig. 5b shows the security triads for Performance RAID node 3.1.1.1. We used the security tools coming with the hardware to configure the countermeasures.

3.2.3. Case Analysis for Production Servers. Last case describes the Servers sub-tree shown in Fig. 6.



(a) Infosec-tree for Storage showing confidentiality, integrity & availability services.

Internal		
(protection, storage, integrity)	→	RAID 5 for SAS Disks RAID 6 for NL-SAS Disks
(protection, storage, availability)	→	RAID 5 for SAS Disks RAID 6 for NL-SAS Disks

(b) Internal triads and countermeasures for infosec-node 3.1.1.1.

Figure 5. Case analysis for storage.

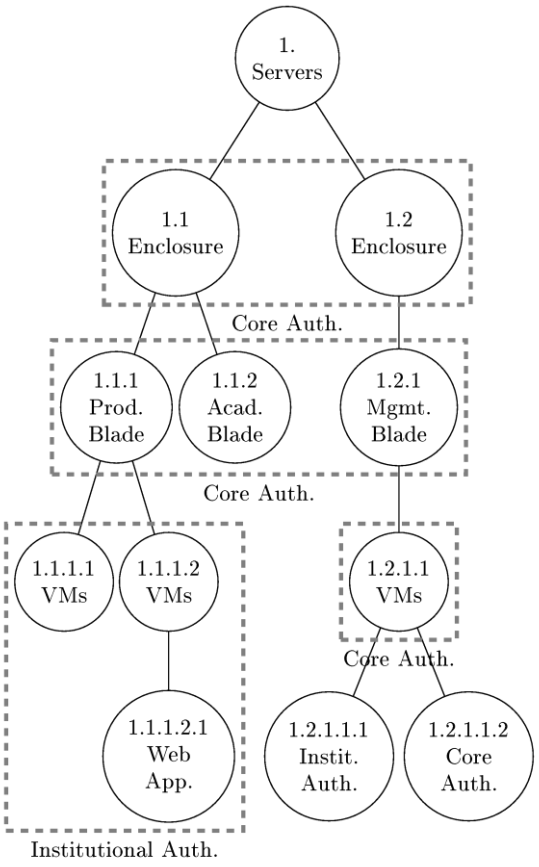


Figure 6. Infosec-tree for servers showing the authentication service.

This example considers authentication requirements (policy 4). The Servers node represents the entire set of blade servers, and it is composed of Enclosures.

. Enclosures are grouping nodes. They are real hardware components, with up to 16 blades each. There are several purposes for servers contained in the Enclosures, namely Production, Academy and Management Servers. The servers contain virtual machines, and the virtual machines provide network services to the users.

Enclosures and Blade Servers can be managed remotely, and we want to apply the authentication policy. We decided to implement two authentication services, one for management the cloud (core authentication), and the other for final users (institutional authentication).

In this example, the authentication servers are also included into the Infosec-tree, because of their inherent complexity, as described in step 4 of the methodology, so they can be target of the assurance process too.

Next section describes different approaches for security information and assurance, which relate to our model and methodology.

4. Related Work

Existing information security concepts, and other security approaches can help to detail the context of the work presented in this paper. We provide an overview of basic security definitions, relevant security models, and industry standards. A comparison of some of these models with the Infosec-tree model is presented in Section 4.3.

4.1. Information Security Models and Standards

Information security is about protecting information for confidentiality, integrity, availability, authenticity, non-repudiation and other additional security goals [7], [13]. Information security policies provide a framework to specify decisions for accessing and protecting information in a system. Moreover, information security models are tools to enforce security policies using formal or informal methods. Security standards capture generalized practices to help reducing the number of successful attacks directed towards information in a system.

ISO/IEC 27000 standard series [14] contain high level guides, with best practices and recommendations for information security management, and they focus on risk and security management for an organization.

Control Objectives for Information and Related Technology (COBIT) [15] incorporates enterprise governance, management techniques, and provides guides for information security and assurance, based on five principles, and seven enablers to achieve the business objectives.

The National Institute of Standards and Technology (NIST) [16], [17] also provides a large number of publications with guidelines, best practices and standards related to computer security.

Some models focus on information security, such as McCumber security model [9]. This model defines a framework for information assurance. It considers security goals (confidentiality, integrity, and availability), information states (processing, storage, and transmission) and security countermeasures (technology, policy and practices, human factors), using a three-dimensional cube to represent potential security goals to be satisfied.

Maconachy [8] proposes a modified version of McCumber model by renaming security goals into security services, adding authentication and non-repudiation to the security services, and a new time dimension for the assurance process.

Table 1: Comparison of standards and security models, in the context of information security.

		Standard or Model					
		ISO/IEC 27000 standard series	COBIT	NIST	Mc-Cumber Maconachy	RMIAS	Infosec-Tree Model
General Features	Focus	*-Risk management -Design and implementation of security countermeasures*	*-Business and information technology governance*	*-Risk management -Design and implementation of security countermeasures -Security for specialized technologies*	*-Risk management -Design and implementation of security countermeasures*	*-Risk management -Design and implementation of security countermeasures*	*-In-depth design and implementation of security countermeasures*
	Paradigm	*-Information security management systems*	*-Planning of information technology processes*	*-Information security management and implementation*	*-Security management and assessment for information technology systems*	*-Information security, assurance management and implementation*	*-Information assurance through applied, in-depth and structured definition of security controls*
	Model structure	*-Standards -Guidelines -Best practices*	*-Standards -Guidelines -Best practices*	*-Standards -Guidelines -Best practices*	*Cube having: -Information states -Information services -Security controls -Time (Maconachy)*	*Four dimension model: -Information System Security Life Cycle -Information Taxonomy -Security Goals -Security Countermeasures*	*Infosec-tree with security countermeasures determined by: -Assurance moment -Information state -Information service*
Detailed Features	Security policies	*-Allows defining security policies*	*-Allows defining security policies*	*-Allows defining security policies*	*-Policies considered in the cube -Facilitates for defining policies*	*-Policies considered in security countermeasures -Facilitates for defining policies*	*-Policies are the input of the methodology*
	Support for implemen-tation	*-Provides tools for implementa-tion*	*-Provides tools for implementa-tion*	*-Provides tools for implementa-tion*	*-Provides tools for implementa-tion*	*-Provides tools for implementa-tion*	*Facilitates in-depth, consistent and structured implementation*
	Assurance moments (protection, detection ,and response)	*-Can be considered and implemented*	*-Supported directly in the model*	*-Supported directly in the model -Also defines identification and recovery*	*-Not defined*	*-Not defined*	*-Supported directly in the model*

Reference Model for Information Assurance & Security (RMIAS) [7] is a related model, which considers information security life cycle, information taxonomy, security goals, and security countermeasures. It also includes details for location, sensitivity, and format, such as paper, electronic, or verbal information.

4.2. Security in Cloud Computing

Regarding to the cloud use cases, we looked for security of large and complex infrastructures. Cloud platforms suffer most challenges and issues found in traditional information technology infrastructures. But they also come with new risks, threats and challenges [18] that may slow down the acceptance as an emerging technology [19].

Academia researchers describe relevant security challenges for clouds [6], [7], [10], [12], [20], [21]. Authors on [20] mention information security as a research issue, while other researchers [10], [11] study the problem using a more theoretical approach.

Important security challenges have been introduced when migrating traditional data centers towards cloud computing, because the conversion process adds new complexities and diminishes the effectiveness of conventional protection mechanisms. For example challenges related to virtualization [3] and authentication technologies [18], [21].

4.3. Comparison of security standards and models

We compared some security models and standards with our Infosec-tree model. Comparison results are shown in Table 1.

We defined two groups of features as the comparison criteria, namely general features (focus, paradigm and model structure), and detailed features (security policies, support for implementation, and assurance moments). The features describe some important difference between the models. The comparison goal is to show differences between models, but we are not looking for a winner standard.

Table 1 shows important benefits of the Infosec-tree Model when compared with existing security models and standards. The assurance process is designed to support practical implementations. The assurance steps are structured, in-depth and consistent, given a pre-defined set of security policies. The methodology can be used to satisfy security requirements for protecting, detecting, or responding to security events.

5. Conclusions

Information security and assurance are complex fields. Assuring large modern technological systems is also complex. We propose a model and a methodology to deal with complexity using a divide-and-conquer idea, and we used a practical tree structure as the main tool.

We applied this idea to our cloud at the university, and the problem became clear and manageable. The methodology provided a convenient tool to deal with the inherent complexity, for information security and the assurance process. The cloud will grow and we expect to keep the assurance process still manageable.

We have also applied the methodology to design security of software applications, mostly for research projects with students, and the process is analogous. Hardware devices, virtual appliances, other components, and their connections become software modules, objects, functions, and interactions between them.

So far, for assuring information, our methodology shows an intuitive and consistent process, independently of the nature of the components managing the information.

Furthermore, the methodology by itself is a documentation system for security requirements and countermeasures, and the documentation structure is also modular enough that it can be updated very easily over time.

6. References

[1] C. Gong, J. Liu, Q. Zhang, H. Chen, and Z. Gong, “The characteristics of cloud computing”, in Parallel Processing Workshops (ICPPW), 2010 39th International Conference on. IEEE, 2010, pp. 275–279.

[2] P. Mell and T. Grance, “The NIST definition of cloud computing”, National Institute of Standards and Technology, vol. 53, no. 6, p. 50, 2009.

[3] T. Erl, R. Puttini, and Z. Mahmood, “Cloud Computing: Concepts, Technology & Architecture”, 1st ed. Upper Saddle River, NJ, USA: Prentice Hall Press, 2013.

[4] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing”, Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1–11, 2011, http://www.sciencedirect.com/science/article/pii/S1084804510001281 (Access Date: 15 Jul, 2014).

[5] T. Dillon, C. Wu, and E. Chang, “Cloud computing: Issues and challenges”, in Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on. IEEE, April 2010, pp. 27–33.

[6] K. Bhamidipati and S. Karanth Shyam, “The need, use and efficiency of trustworthy security model in cloud computing for information assurance”, in Cloud Computing Technologies, Applications and Management (ICCCTAM), 2012 International Conference on. IEEE, 2012, pp. 69–73.

[7] Y. Cherdantseva and J. Hilton, “A reference model of information assurance & security”, in Availability, Reliability and Security (ARES), 2013 Eighth International Conference on. IEEE, 2013, pp. 546–555.

[8] W. V. Maconachy, C. D. Schou, D. Ragsdale, and D. Welch, "A model for information assurance: An integrated approach", in Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, vol. 310. New York, USA, 2001.
[9] J. McCumber, "Information systems security: A comprehensive model", in Proceedings of the 14th National Computer Security Conference, 1991.
[10] S. Ristov, M. Gusev, and M. Kostoska, "A new methodology for security evaluation in cloud computing", in MIPRO, 2012 Proceedings of the 35th International Convention. IEEE, 2012, pp. 1484–1489.
[11] L. B. A. Rabai, M. Jouini, A. B. Aissa, and A. Mili, "A cybersecurity model in cloud computing environments", Journal of King Saud University - Computer and Information Sciences, vol. 25, no. 1, pp. 63 – 75, 2013, http://www.sciencedirect.com/science/article/pii/ S131915781200033X (Access Date: 2 Aug, 2014).
[12] K. S.O., I. F., and O. Awodele, "Cloud computing security issues and challenges", International Journal of Computer Networks, 2011.
[13] M. Bishop, "Computer security: art and science", Addison-Wesley, 2002.
[14] ISO, "ISO 27005:2008 Information technology – Security techniques – Information security risk management", ISO, 2008.
[15] Information Systems. Audit and Control Association, "COBIT 5 for Information Security Std.", 2013.
[16] National Institute of Standards and Technology, "FIPS 46-3: Data encryption standard", Federal Information Processing Standards, National Bureau of Standards, US Department of Commerce, 1999.
[17] National Institute of Standards and Technology, "FIPS 140-2: Security requirements for cryptographic modules", Federal Information Processing Standards, National Bureau of Standards, US Department of Commerce, 2001.
[18] S. Mansfield-Devine, "Danger in the clouds", Network Security, vol. 2008, no. 12, pp. 9 – 11, 2008. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1353485808701405 (Access Date: 23 Jun, 2014).
[19] F. Gens. (2009, December) "New idc it cloud services survey: Top benefits and challenges". IDC eXchange. [Online]. Available: http://blogs.idc.com/ie/?p=730 (Access Date: 02 Aug, 2014)
[20] M. Ahmed, A. S. M. R. Chowdhury, M. Ahmed, and M. M. H. Rafee, "An advanced survey on cloud computing and state-of-the-art research issues", IJCSI International Journal of Computer Science Issues, vol. 9, no. 1, January 2012.
[21] D. Zissis and D. Lekkas, "Addressing cloud computing security issues", Future Generation Computer Systems, vol. 28, no. 3, pp. 583 – 592, 2012, http://www.sciencedirect.com/science/article/pii/S0167739X10002554 (Access Date: 23 Jun, 2014).
[22] R. Bejtlich, "The Tao of Network Security Monitoring: Beyond Intrusion Detection", Pearson Education, 2004.
[23] E. Fernandez-Buglioni, "Security Patterns in Practice: Designing Secure Architectures Using Software Patterns", 1st ed. Wiley Publishing, 2013.
[24] R. Villalón, B.Solano, and G.Marín, "An Applied Methodology for Information Security and Assurance", International Conference for Internet Technology and Secured Transactions, 2014.
[25] V. Arora, "Comparing different information security standards: COBIT v s. ISO 27001, 2010", [Online]. Available: https://qatar.cmu.edu/media/assets/CPUCIS2010-1.pdf (Access Date: 27 Dec, 2014)

7. Acknowledgements

We would like to acknowledge the entire university personnel participant in any form in the CITIC-ECCI Research Project 834-B3-145 "Creación de la Nube Académica Computacional de la UCR" for the continuous support and hard work.

